

Ordonnance sur le dossier électronique du patient (ODEP)

du 22 mars 2017 (État le 1^{er} octobre 2024)

Le Conseil fédéral suisse,

vu la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP)¹,
arrête:

Chapitre 1 Niveaux de confidentialité et droits d'accès

Art. 1 Niveaux de confidentialité

¹ Le patient peut attribuer aux données médicales de son dossier électronique l'un des trois niveaux de confidentialité suivants:

- a. normal;
- b. restreint;
- c. secret.

² À défaut, les nouvelles données enregistrées dans le dossier électronique du patient ont le niveau de confidentialité «normal», sauf si le professionnel de la santé leur attribue le niveau de confidentialité «restreint».

Art. 2 Droits d'accès

¹ Le patient peut accorder à des professionnels de la santé ou à des groupes de professionnels de la santé un droit d'accès au niveau de confidentialité «normal» ou aux niveaux de confidentialité «normal» et «restreint».

² En cas d'urgence médicale, les professionnels de la santé peuvent accéder aux données du niveau de confidentialité «normal» même sans avoir reçu de droit d'accès. Le patient doit être informé d'un accès d'urgence dans un délai approprié.

³ Le professionnel de la santé qui intègre un groupe reçoit les droits d'accès accordés à ce groupe. Ces droits lui sont retirés lorsqu'il quitte le groupe.

Art. 3 Durée des droits d'accès

¹ Les droits d'accès des professionnels de la santé sont accordés jusqu'à leur suppression par le patient.

² Les droits d'accès des groupes de professionnels de la santé sont accordés pour une durée fixée par le patient.

RO 2017 2211

¹ RS 816.1

Art. 4 Options données au patient

Le patient peut:

- a. choisir le niveau de confidentialité attribué aux nouvelles données enregistrées dans son dossier;
- b. refuser tout accès à son dossier électronique à certains professionnels de la santé;
- c. choisir d'être informé que des professionnels de la santé intègrent un groupe auquel il a accordé un droit d'accès;
- d. limiter la durée des droits d'accès des professionnels de la santé à son entière discrétion;
- e. prévoir l'extension du droit d'accès au niveau de confidentialité «restreint» en cas d'urgence médicale ou refuser tout accès à son dossier électronique en tel cas;
- f. désigner un représentant;
- g. autoriser des professionnels de la santé affiliés à sa communauté de référence à accorder à d'autres professionnels de la santé ou à d'autres groupes de professionnels de la santé tout au plus les mêmes droits d'accès que ceux qu'il leur a attribués.

Chapitre 2 Numéro d'identification du patient**Art. 5** Format

¹ Le numéro d'identification du patient se compose d'un numéro de base, d'un numéro d'identification et d'une clé de contrôle. Il ne doit en aucun cas permettre de tirer des conclusions sur le patient.

² Le Département fédéral de l'intérieur (DFI) fixe les prescriptions relatives à la composition du numéro d'identification du patient et au calcul de la clé de contrôle.

Art. 6 Demande d'attribution

¹ Le numéro d'identification du patient est attribué par la Centrale de compensation (CdC) à la demande d'une communauté de référence.

² À cet effet, la communauté de référence communique à la CdC les données suivantes concernant le patient:

- a. nom;
- b. prénoms;
- c. sexe;
- d. date de naissance;

e.² numéro AVS.

³ Si les données communiquées ne sont pas suffisantes pour attribuer un numéro d'identification, la CdC peut demander des données complémentaires à la communauté de référence.

Art. 7 Consultation et saisie

¹ Les communautés et les communautés de référence peuvent demander le numéro d'identification des patients auprès de la CdC par voie électronique.

² Toute saisie manuelle du numéro d'identification du patient requiert une vérification de la clé de contrôle.

Art. 8 Annulation

¹ Si le dossier électronique d'un patient est supprimé, son numéro d'identification est annulé dans la banque de données d'identification de la CdC.

² La CdC informe la communauté ou la communauté de référence concernée de l'annulation du numéro d'identification du patient.

³ Un numéro d'identification annulé ne peut plus être attribué.

Chapitre 3 Communautés et communautés de référence

Section 1 Communautés

Art. 9 Identificateur d'objet et gestion

¹ Les communautés doivent demander un identificateur d'objet (OID) au service de recherche de l'OID visé à l'art. 42, pour elles-mêmes et pour les institutions de santé qui leur sont affiliées.

² Elles sont tenues de gérer les institutions de santé, les professionnels de la santé et les groupes de professionnels de la santé qui leur sont affiliés. À cet effet, elles doivent en particulier:

- a. régler les modalités d'entrée et de sortie;
- b. identifier les professionnels de la santé et vérifier leurs qualifications professionnelles;
- c. attribuer aux groupes de professionnels de la santé un OID qui se fonde sur celui de l'institution de santé;
- d. assurer la mise à jour des données dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41;

² Nouvelle teneur selon l'annexe ch. II 32 de l'O du 17 nov. 2021, en vigueur depuis le 1^{er} janv. 2022 (RO 2021 800).

- e. veiller à ce que les professionnels de la santé accèdent au dossier électronique du patient en s'authentifiant avec un moyen d'identification émis par un éditeur certifié au sens de l'art. 31;
- f. informer les patients, à leur demande, lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé.

Art. 10 Tenue et transfert des données

¹ Les communautés doivent:

- a. veiller à l'application des art. 1 et 2, al. 2;
- b. veiller à ce que les données médicales des dossiers électroniques soient sauvegardées séparément des autres données;
- c. veiller à ce que le procédé de chiffrement utilisé pour l'enregistrement et le transfert des données soit conforme aux progrès techniques;
- d. veiller à ce que les données saisies dans le dossier électronique du patient par les professionnels de la santé soient détruites au bout de vingt ans;
- e. veiller, en cas de suppression du dossier électronique en application de l'art. 21, à ce que toutes les données du dossier soient détruites.

² À la demande du patient, elles doivent veiller au surplus à ce que:

- a. certaines données médicales le concernant ne soient pas enregistrées dans son dossier électronique;
- b. des données soient exclues de la procédure de destruction visée à l'al. 1, let. d;
- c. certaines données médicales le concernant figurant dans son dossier électronique soient détruites.

³ Le DFI fixe les prescriptions techniques et organisationnelles relatives à la tenue et au transfert des données du dossier. Il règle en particulier:

- a. les métadonnées à utiliser;
- b. les formats d'échange à utiliser;
- c. les profils d'intégration à utiliser;
- d. les prescriptions relatives aux historiques.

⁴ Il peut décider de faire publier les prescriptions visées à l'al. 3 dans la langue d'origine et de ne pas les faire traduire dans les autres langues officielles.

⁵ Il peut habiliter l'Office fédéral de la santé publique (OFSP) à adapter aux progrès techniques les prescriptions visées à l'al. 3.

Art. 11 Portail d'accès pour les professionnels de la santé

Le DFI fixe les exigences applicables au portail d'accès destiné aux professionnels de la santé, notamment pour la mise à disposition et la consultation des données ainsi que pour l'accessibilité.

Art. 12 Protection et sécurité des données

¹ Les communautés doivent se doter d'un système de gestion de la protection et de la sécurité des données adapté aux risques. Ce système doit comprendre les éléments suivants en particulier:

- a. un système de détection et de gestion des incidents de sécurité;
- b.³ un inventaire des moyens informatiques et un registre des activités de traitement;
- c. les exigences relatives à la protection et à la sécurité des données imposées aux institutions de santé et aux tiers affiliés à la communauté.

² Les communautés désignent un responsable de la protection et de la sécurité des données.

³ Elles sont tenues de signaler à l'OFSP tout incident ayant une influence sur la sécurité survenu dans le système de gestion de la protection et de la sécurité des données.

⁴ Le DFI fixe les exigences techniques et organisationnelles applicables à la protection et à la sécurité des données.

⁵ Les supports de données doivent se trouver en Suisse et être régis par le droit suisse.

Art. 13 Service d'assistance pour les professionnels de la santé

Les communautés doivent désigner un service d'assistance chargé d'aider les professionnels de la santé à utiliser le dossier électronique.

Section 2 Communautés de référence**Art. 14** Exigences supplémentaires à l'égard des communautés de référence

Les communautés de référence doivent observer les prescriptions énoncées dans la présente section en plus de celles énoncées dans la section 1.

Art. 15 Information du patient

¹ Avant d'ouvrir un dossier électronique, la communauté de référence est tenue d'informer le patient sur les points suivants en particulier:

- a. le but du dossier électronique;
- b. le traitement des données;
- c. les conséquences du consentement, la possibilité de le révoquer et les conséquences de la révocation;
- d. l'attribution des droits d'accès.

³ Nouvelle teneur selon l'annexe 2 ch. II 106 de l'O du 31 août 2022 sur la protection des données, en vigueur depuis le 1^{er} sept. 2023 (RO 2022 568).

² Elle doit recommander au patient des mesures de protection et de sécurité des données.

Art. 16⁴ Consentement

La communauté de référence doit obtenir le consentement du patient à la constitution d'un dossier électronique. La déclaration de consentement doit:

- a. porter la signature manuscrite du patient ou sa signature électronique qualifiée arborant un horodatage qualifié au sens de la loi du 18 mars 2016 sur la signature électronique⁵, ou
- b. être confirmée par le patient à l'aide d'un moyen d'identification émis par un éditeur certifié au sens de l'art. 31.

Art. 17 Gestion

¹ Les communautés de référence doivent:

- a. régler les modalités d'ouverture, de gestion et de suppression du dossier électronique;
- b. identifier les patients;
- c. veiller à ce que les patients et leurs représentants accèdent au dossier électronique en s'authentifiant avec un moyen d'identification émis par un éditeur certifié au sens de l'art. 31;
- d. demander les numéros d'identification des patients;
- e. prévoir des procédures régissant le changement de communauté de référence.

² Elles doivent veiller à la mise en œuvre de l'art. 2, al. 1 et 3, et des art. 3 et 4.

Art. 18 Portail d'accès destiné aux patients

Le DFI fixe les exigences applicables au portail d'accès destiné aux patients, en particulier:

- a. pour la mise en œuvre des art. 1 à 4, notamment la présentation de la composition des groupes de professionnels de la santé;
- b. pour la présentation des historiques;
- c. pour la saisie et la consultation de données;
- d. pour l'accessibilité.

Art. 19 Données saisies par les patients

Le DFI fixe les exigences applicables à l'utilisation des données médicales saisies par les patients.

⁴ Nouvelle teneur selon l'art. 8 ch. 1 de l'O du 28 août 2024 sur les aides financières pour le dossier électronique du patient, en vigueur depuis le 1^{er} oct. 2024 (RO 2024 461).

⁵ RS 943.03

Art. 20 Service d'assistance pour les patients

Les communautés de référence doivent désigner un service d'assistance chargé d'aider les patients à utiliser leur dossier électronique.

Art. 21 Suppression du dossier électronique du patient

¹ La communauté de référence supprime le dossier électronique du patient lorsque le patient révoque son consentement à la tenue du dossier électronique. La déclaration de révocation doit être conservée pendant dix ans.

² La communauté de référence peut supprimer un dossier électronique au plus tôt deux ans après le décès du patient.

³ Lorsqu'une communauté de référence a supprimé un dossier électronique du patient, elle doit, dans un délai approprié, supprimer tous les droits d'accès au dossier et informer toutes les communautés ainsi que la CdC.

Section 3 Évaluation et recherche**Art. 22**

¹ Les communautés et les communautés de référence sont tenues de mettre régulièrement à la disposition de l'OFSP des données utilisant des pseudonymes pour l'évaluation visée à l'art. 18 LDEP.

² Le DFI fixe les données à fournir et les délais.

³ L'OFSP peut traiter les données visées à l'art. 39 à des fins d'évaluation et de recherche.

⁴ Il peut demander aux organismes de certification ou aux organismes titulaires d'un certificat les documents nécessaires à la certification ou au renouvellement de la certification.

Chapitre 4 Moyens d'identification**Art. 23** Exigences applicables

Le moyen d'identification doit:

- a. satisfaire au niveau de confiance 3 de la norme ISO/IEC 29115:2013(E)⁶;
- b. être conçu de manière à ce que seule la personne autorisée puisse l'utiliser;
- c. utiliser une procédure d'authentification conforme aux progrès techniques comportant au moins deux facteurs d'authentification;

⁶ La norme peut être obtenue contre paiement auprès de l'Association suisse de normalisation (www.snv.ch) ou être consultée gratuitement auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne.

- d. avoir une durée de validité de cinq ans au maximum.

Art. 24 Vérification d'identité

¹ L'éditeur est tenu de vérifier l'identité de la personne qui demande un moyen d'identification. Pour établir son identité, le demandeur doit présenter un document d'identité au sens de la loi du 22 juin 2001 sur les documents d'identité⁷ ou un titre de séjour au sens des art. 41 à 41b de la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration⁸ ou encore déposer par voie électronique une demande sur laquelle est apposée une signature électronique qualifiée au sens de la loi du 18 mars 2016 sur la signature électronique⁹.

² La vérification de l'identité des demandeurs peut être déléguée à des tiers.

Art. 25 Données

¹ L'éditeur du moyen d'identification attribue au demandeur un identificateur univoque.

² Il assigne au demandeur les données suivantes en se fondant sur la pièce d'identité fournie conformément à l'art. 24, al. 1:

- a. nom;
- b. prénoms;
- c. sexe;
- d. date de naissance;
- e. numéro de la pièce d'identité fournie.

³ Si le moyen d'identification est également utilisé comme preuve des qualifications professionnelles, l'éditeur doit assigner au professionnel de la santé concerné les données supplémentaires suivantes:

- a. le numéro d'identification (GLN¹⁰) univoque;
- b. les qualifications professionnelles contrôlées à l'aide d'un registre fédéral ou cantonal.

⁴ Il peut transmettre les données visées aux al. 1, 2, let. a à d, et 3 à des fins d'identification aux communautés et aux communautés de référence.

⁵ Il informe le demandeur des dispositions de sécurité à respecter lors de l'utilisation du moyen d'identification.

⁶ Il sauvegarde les données sur des supports de données qui doivent se trouver en Suisse et être régis par le droit suisse.

⁷ RS 143.1

⁸ RS 142.20. Le titre a été adapté au 1^{er} janv. 2019 en application de l'art. 12 al. 2 de la LF du 18 juin 2004 sur les publications officielles (RS 170.512).

⁹ RS 943.03

¹⁰ GLN est l'acronyme de *Global Location Number* (numéro d'identification mondial).

Art. 26 Renouvellement

¹ Le moyen d'identification peut être renouvelé avant son expiration.

² Avant de renouveler le moyen d'identification, l'éditeur vérifie l'identité du demandeur.

Art. 27 Blocage

Le titulaire d'un moyen d'identification peut à tout moment ordonner le blocage temporaire ou définitif du moyen d'identification.

Chapitre 5 Accréditation**Art. 28** Critères

¹ L'organisme de certification d'une communauté, d'une communauté de référence ou d'un portail d'accès doit être reconnu apte à l'audit et à la certification de systèmes de management par l'un des organismes suivants:

- a. le Service d'accréditation suisse au sens de l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation¹¹;
- b. un organisme d'accréditation étranger membre de l'organisation European co-operation for Accreditation;
- c. un organisme d'accréditation reconnu par la Suisse en vertu d'un traité international.¹²

² L'organisme de certification des éditeurs de moyens d'identification doit être reconnu apte à l'audit et à la certification de produits, de procédures et de services par un des organismes visés à l'al. 1, let. a, b ou c.¹³

³ L'organisme de certification doit disposer d'une organisation et d'une procédure de contrôle déterminées. Les points suivants doivent notamment être réglés:

- a. les critères utilisés pour vérifier le respect des critères de certification;
- b. le déroulement de la procédure, notamment en cas de constat d'irrégularités.

⁴ L'organisme de certification doit utiliser le système de certification fourni par l'OFSP pour l'examen du transfert des données entre communautés et communautés de référence.

⁵ Le DFI fixe les exigences minimales applicables à la qualification du personnel qui réalise les certifications.

¹¹ RS 946.512

¹² Nouvelle teneur selon le ch. I de l'O du 31 janv. 2018, en vigueur depuis le 1^{er} mars 2018 (RO 2018 717).

¹³ Nouvelle teneur selon le ch. I de l'O du 31 janv. 2018, en vigueur depuis le 1^{er} mars 2018 (RO 2018 717).

Art. 29 Procédure

Le Service d'accréditation suisse fait appel à l'OFSP pour la procédure d'accréditation ainsi que pour le contrôle, la suspension ou le retrait d'une accréditation.

Chapitre 6 Certification**Section 1 Critères****Art. 30** Communautés et communautés de référence

¹ Une certification est délivrée aux communautés qui remplissent les critères fixés aux art. 9 à 13 et aux communautés de référence qui remplissent les critères fixés aux art. 9 à 21.

² Le DFI concrétise les critères de certification fixés aux art. 9 à 21.

³ Il peut habiliter l'OFSP à adapter aux progrès techniques les critères visés à l'al. 2.

Art. 31 Éditeurs de moyens d'identification

¹ Une certification est délivrée aux éditeurs de moyens d'identification qui répondent aux conditions suivantes:

- a. ils sont en mesure d'émettre et d'administrer des moyens d'identification en respectant les exigences fixées aux art. 23 à 27;
- b. ils veillent à ce que leur personnel possède les connaissances techniques, l'expérience et les qualifications requises;
- c. ils utilisent des systèmes et des produits informatiques fiables et les exploitent de manière sûre;
- d. ils garantissent la protection et la sécurité des données par des mesures organisationnelles et techniques appropriées et assurent les contrôles correspondants.

² Le DFI concrétise les critères de certification fixés aux art. 23 à 27.

³ Il peut habiliter l'OFSP à adapter aux progrès techniques les critères visés à l'al. 2.

Section 2 Procédure de certification**Art. 32** Déroulement

¹ L'organisme de certification vérifie sur la base de la documentation du demandeur si celui-ci est préparé à l'audit de certification.

² Dans l'audit de certification, il vérifie que les critères de certification sont remplis.

³ Il délivre le certificat à la communauté, à la communauté de référence ou à l'éditeur de moyens d'identification qui remplit les exigences requises.

⁴ Un nouvel audit de certification conforme aux prescriptions de l'al. 2 doit être réalisé avant l'expiration du certificat (renouvellement de la certification).

Art. 33 Communication et publication des certificats délivrés

¹ L'organisme de certification communique à l'OFSP tous les cas de certification, de renouvellement de la certification, de suspension ou de retrait de certificat et fournit les données requises pour la saisie dans le service de recherche des communautés et communautés de référence visé à l'art. 40.

² L'OFSP publie un registre des certificats délivrés.

Art. 34 Procédure de vérification

¹ L'organisme de certification est tenu de vérifier chaque année si les critères de certification sont toujours remplis.

² S'il constate au cours de la procédure de vérification des écarts substantiels par rapport aux critères de certification, notamment concernant le respect de conditions ou de charges, il en informe l'OFSP.

Art. 35 Durée de validité

Le certificat est établi pour une durée de trois ans.

Art. 36 Obligation de signaler les adaptations techniques ou organisationnelles substantielles

¹ Les communautés, les communautés de référence et les éditeurs de moyens d'identification sont tenus de signaler à l'organisme de certification toutes les adaptations techniques ou organisationnelles substantielles.

² L'organisme de certification décide si les adaptations qui lui sont signalées sont examinées dans le cadre de la procédure de vérification, d'un renouvellement ordinaire de la certification ou d'un renouvellement extraordinaire de la certification.

Art. 37 Clause de sauvegarde

¹ En cas de grave mise en danger de la protection ou de la sécurité des données du dossier électronique du patient, l'OFSP peut:

- a. refuser provisoirement à des communautés et communautés de référence l'accès au dossier électronique du patient;
- b. interdire l'utilisation de certains moyens d'identification pour accéder au dossier électronique du patient;
- c. ordonner un renouvellement extraordinaire de la certification.

² Il peut demander à l'organisme de certification ou à l'organisme titulaire d'un certificat les documents nécessaires à la certification ou à un renouvellement de la certification.

Section 3 Sanctions

Art. 38

¹ L'organisme de certification peut suspendre ou retirer un certificat s'il constate des défaillances graves au cours de la procédure de vérification prévue à l'art. 34. Il y a défaillance grave dans les cas suivants notamment:

- a. des critères de certification substantiels ne sont plus remplis;
- b. un certificat est utilisé fallacieusement ou abusivement.

² En cas de litige concernant une suspension ou un retrait, l'évaluation et la procédure sont régies par les dispositions du droit civil applicables aux relations contractuelles entre l'organisme de certification et la communauté, la communauté de référence ou l'éditeur de moyens d'identification titulaire du certificat concerné.

³ L'OFSP peut ordonner à l'organisme de certification de procéder à une vérification s'il a de sérieuses raisons de penser qu'une communauté, une communauté de référence ou un éditeur de moyens d'identification titulaire d'un certificat ne remplit pas les critères de certification.

Chapitre 7 Services de recherche de données

Section 1 Généralités

Art. 39

¹ L'OFSP exploite les services de recherche suivants:

- a. service de recherche des communautés et des communautés de référence;
- b. service de recherche des institutions de santé et des professionnels de la santé autorisés à traiter les données du dossier électronique;
- c. service de recherche des métadonnées (art. 10, al. 3, let. a);
- d. service de recherche des OID enregistrés pour le dossier électronique.

Section 2 Contenu

Art. 40 Service de recherche des communautés et communautés de référence

¹ Le service de recherche des communautés et des communautés de référence contient les données suivantes sur chacune d'entre elles:

- a. leur désignation;
- b. leur OID;
- c. le certificat assurant une authentification sûre par rapport aux autres communautés et communautés de référence;

d. l'adresse Internet de leur point d'accès.

² L'OFSP saisit dans le service de recherche les données fournies en vertu de l'art. 33, al. 1.

Art. 41 Service de recherche des institutions de santé et des professionnels de la santé

¹ Les communautés et les communautés de référence saisissent les données suivantes dans le service de recherche des institutions de santé et des professionnels de la santé:

- a. pour les institutions de santé et les groupes de professionnels de la santé:
 1. leur désignation et leur adresse,
 2. leur OID,
 - 3.¹⁴ ...
- b. pour les professionnels de la santé:
 1. leur identité,
 - 2.¹⁵ le GLN,
 3. la désignation et l'adresse des institutions de santé dans lesquelles ils travaillent ou des groupes de professionnels de la santé auxquels ils appartiennent.

² Le DFI peut définir des données supplémentaires que les communautés et les communautés de référence doivent saisir dans le service de recherche.

Art. 42 Service de recherche de l'OID

Le service de recherche de l'OID gère l'OID des communautés, des communautés de référence et des institutions de santé qui leur sont affiliées.

Art. 43 Émoluments

¹ L'OFSP perçoit un émolument forfaitaire annuel de 40 000 francs auprès des communautés et des communautés de référence pour la mise à disposition des services de recherche.

² Au surplus, les dispositions de l'ordonnance générale du 8 septembre 2004 sur les émoluments¹⁶ sont applicables.

¹⁴ Abrogé par le ch. I de l'O du 8 mars 2019, avec effet au 1^{er} avr. 2019 (RO **2019** 937).

¹⁵ Nouvelle teneur selon le ch. I de l'O du 31 janv. 2018, en vigueur depuis le 1^{er} mars 2018 (RO **2018** 717).

¹⁶ RS **172.041.1**

Chapitre 8 Entrée en vigueur**Art. 44**

La présente ordonnance entre en vigueur le 15 avril 2017.